Protection Approaches Based on Critical Locations in Optical Backbone Networks Under Large-scale Malicious Attacks

STSM Applicant: Ayşegül Yayımlı (MC Member Turkey), Istanbul Technical University
Host: Lena Wosinska, ONLab, Royal Institute of Technology (KTH), Sweden

Period: December 15th 2016 – December 23rd 2016
Working group: WG4

1. Purpose of the STSM

In a communication network, the underlying physical topology that carries the traffic plays a very important role in providing survivable services. The performance of the whole network is affected by failures of its individual components. Understanding and modeling the behavior of a typical realistic optical backbone network under a large-scale malicious attack, where multiple nodes and/or edges fail, can allow us to identify critical locations in the network. As attacks may be geographically uncorrelated or exhibit various behaviors and patterns, criticality of locations may be different for different attack methods. Information of location criticality can be used to limit the impact of the attacks as well as to design better protection methods, and better reactive approaches for network recovery.

Our aim in this STSM was to discuss, define and compare new metrics that could be used in communication networks, and to develop new approaches to measure the criticality of network components (nodes and/or edges) that may be targeted by malicious attacks. Based on our studies, we aim to design new protection approaches against such multiple sequential or simultaneous deliberate failures. We mainly focus on optical backbone networks of continent-scale where several nodes may host data-centers. The proliferation of data centers and cloud computing introduces drastic changes into traffic patterns, so a part of our study is aiming at analyzing network performance under different traffic patterns.

In the next phase, we will continue our collaboration to explore methods and algorithms to update the network topology, and to better design node locations (e.g. data centers) to increase availability and reduce the network vulnerability.

Our work in this STSM is directly related to the following outcomes expected from RECODIS action:
- new measures to evaluate the vulnerability of networks to disruption,
- methods to update network topology to reduce its vulnerability to disaster-based failures.

2. Description of the work and preliminary results

Before the STSM started, we made some pre-study by reviewing the metrics that were used in literature. Various metrics that could be of interest for our studies were found in studies related to transportation networks (railroad and motorways), and power grids[1-5]. These metrics can be implemented and/or adapted to communication networks, as the general network studies show important similarities.

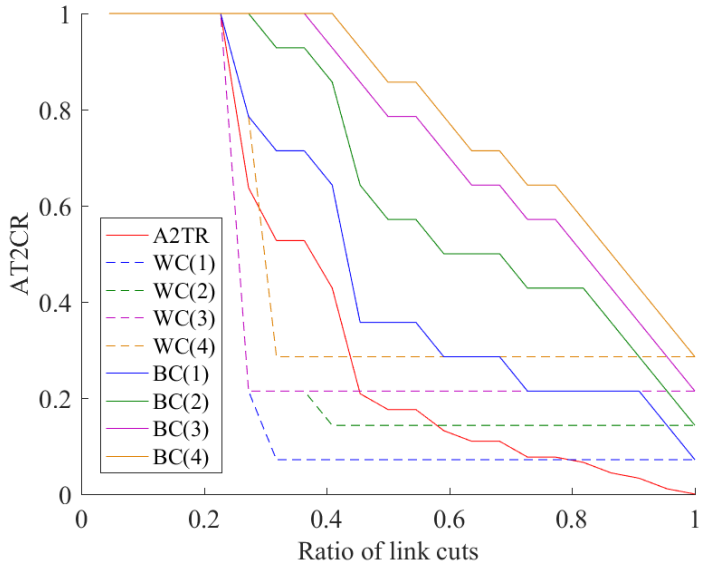
We conducted several telco meetings to define a framework of our studies. The traffic model, the network topologies to be used, the metrics that we could use from earlier studies[1-6], the attack model and what type of attacks to include in our studies during STSM were discussed during those meetings. The following metrics were examined: assortative coefficient, centrality measures, average two terminal reliability (ATTR), vulnerability measures for nodes and the network,

accessibility, Hansen accessibility index, and remoteness index. Some of these metrics need to be adapted to communication networks before they can be applied.

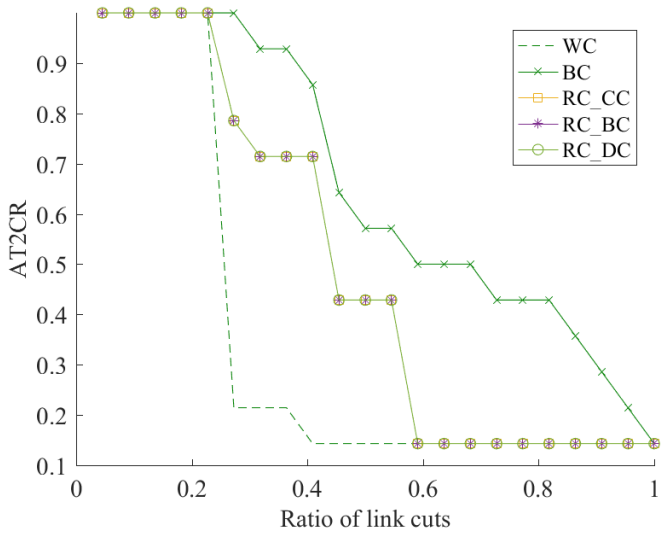
We also discussed the effects of how the different measurement methods and different network routing models affect the outcome of the criticality ranking of network elements. Similarly, different traffic models can affect the ranking. Our results show that when measuring the vulnerability and criticality of the network elements, one should carefully design the simulations, and be meticulous about the implementation details such as routing and resource assignment policy, and how to resolve the ties.

During the STSM period, we decided that our efforts should be first focused on communication networks with datacenters, since the inter-datacenter network survivability under large scale attacks were not considered sa far in terms of accessibility and vulnerability metrics. It is important to analyze the network properly with carefully selected metrics, since using metrics that were designed to measure a different type of traffic and network property can be misleading.

Our preliminary results where we consider simultaneous or sequential link-cuts show that the metrics such as ATTR are not able to capture the vulnerabilities of inter-datacenter networks. In many cases, these metrics underestimate or overestimate the node vulnerabilities. Hence, we proposed a new metric to measure the vulnerability of nodes in inter-datacenter networks. Our results are very promising and we also defined upper and lower bounds for node vulnerabilities. Our results show that inter-datacenter network vulnerability is better measured with the new metric, which takes into account the number and location of datacenters, as opposed to existing metrics which do not consider datacenters. We were able to show this results through several numerical examples that were run on both small and large continent-scale backbone networks.



As an example of how our calculations to measure the best and worst case network vulnerability in terms of accessibility of the nodes having datacenters, we performed simulations over different networks. The results taken from one network is shown in the figure above. Here, the x axis shows the percentage of the links cut by the attacker, and the y axis shows the average two terminal reliability, worst case (WC) and best case (BC) vulnerabilities when there are one to four replica of the data in the network. This figure clearly shows that for inter-datacenter networks, we need new metrics to represent the vulnerability of the network, because metrics such as ATTR are not capable to capture the dynamics of these networks.



We also studied the different placement models for the replicas in a network, and how they affect the overall vulnerability. The second figure shows the results of a small size topology (continent-scale, but small number of nodes). Again, here, the x axis shows the percentage of the links cut by the attacker, and the y axis shows worst case (WC) and best case (BC) vulnerabilities when there are two replica of the data in the network, and the actual vulnerabilities when three different datacenter placement methods are used.

Further results of networks of different topologies will be presented on the RECODIS WG4 meeting in February 2017 in Wroclaw.

After the STSM we continue to work on metrics, focusing on different aspects such as attacks on the nodes, and/or on the links. We are also planning to include the traffic layer simulations in our model, to be able to analyze the network behavior in a more realistic scenario. This will also provide us more information on developing a protection/restoration approach against such large-scale malicious attacks.

4. Future collaboration with the Host institution

We consider the STSM as a very successful start of a fruitful collaboration in the frame of WG4. We are going to continue our study described above, with the aim of publishing our results in two conference papers. In addition we are also planning a visit of Carlos Natalino Silva (postdoc at ONLab) to Istanbul Technical University in the spring of 2017 to work on the planned journal paper.

There are many directions that could be taken in this topic for future studies. We will continue our collaboration with the ONLab to further investigate potential problems on this topic. As stated above, we also plan to explore methods and algorithms to update the network topology to increase availability of nodes and to reduce the overall network vulnerability.

During the visit to ONLab, we also had a meeting where we discussed ideas about possible research project proposals whose focus is extending the problems of this STSM.

5. Foreseen publications/articles resulting from the STSM

We are planning two conference papers and a journal article to publish the outcomes of this STSM, and the related planned work for the near future. The targeted conferences are ONDM 2017 and RNDM 2017. A journal article will be prepared by the fall of 2017.

References

[1] A. T. Murray, T. H. Grubesic, "Critical Infrastructure: Reliability and Vulnerability", Springer-Verlag, Helderberg, 2007.
[2] S. S. Chopra, T. Dillon, M. M. Bilec, V. Khanna, " A Network-based framework for assessing infrastructure resilience: A case study of the London metro system", J. R. Soc. Interface 13: 20160113. http://dx.doi.org/10.1098/rsif.2016.0113
[3] J. Ko, S. Lee, T. Shon, "Towards a novel quantification approach based on smart grid network vulnerability score", Int. J. on Energy Research, V. 40, pp. 298--312, July 2015.
[4] J. Zhang, F. Hu, S. Wang, Y. Dai, Y. Wang, "Structural vulnerability and intervention of high speed railway networks", Physica A: Statistical Mechanics and its Applications, V. 462, pp. 743--751, Nov. 2016.
[5] S.S. Chopra, T. Dillon, M. M. Bilec, V. Khanna, “A network-based framework for assessing infrastructure resilience: a case study of the London metro system. J. R. Soc. Interface 13: 20160113. http://dx.doi.org/10.1098/rsif.2016.0113
[6] J. Rak, K. Walkowiak, “Reliable anycast and unicast routing: protection against attacks”, Telecommun. Systems, 52:889–906, 2013.